

# Robust Security Features

**Comprehensive, Active,  
and Compliant Security—**  
*Powered by Azure*

The Previstar® Continual Preparedness System™ comprises all four modules, seamlessly integrated to form the ultimate end-to-end preparedness system for strategic planning and real-time application.



## Network Isolation & Traffic Control (VNet + NSGs)

- Both VMs live in the same **Virtual Network (VNet)** but on **separate subnets**:
  - › WebSubnet → IIS/ASP.NET V
  - › DBSubnet → SQL Server VM
- Network Security Groups (NSGs) are locked down:
  - › **IIS VM**: Only **443 (HTTP/HTTPS)** open to public, **3389 (RDP)** only via Azure Bastion
  - › **SQL VM**: 1433 (SQL) **open only from IIS VM's subnet** — no public endpoint
- **Azure DDoS Protection Standard** is enabled on the VNet — protecting our web app from volumetric attacks.



## Identity & Access Control (RBAC + Managed Identities)

- We use **Azure Role-Based Access Control (RBAC)** with least privilege:
  - › Devs: Virtual Machine Contributor (only for their VMs)
  - › Admins: Reader + JIT access
- Our **ASP.NET app uses Azure Managed Identity** to securely pull:
  - › SQL connection string
  - › API keys
  - › Certificates → **No secrets in web.config**
- **Azure AD Login** is enabled for both VMs — no local accounts, no passwords in RDP.



## Encryption at Rest & In Transit

- **Azure Disk Encryption** is enabled on **both VMs**:
  - › Data disks encrypted with **customer-managed keys (CMK)** in **Azure Key Vault**
- **MS SQL Server Database**:
  - › **Transparent Data Encryption (TDE)** → database files encrypted
  - › **Always Encrypted** for PII columns
- **TLS 1.2+ enforced** between IIS and SQL:
- **Key Vault** stores all secrets — rotated every 90 days.



## Threat Detection & Monitoring (Defender for Cloud)

- **Microsoft Defender for Cloud** is enabled and active:
  - › **Defender for Servers**: Antimalware + EDR on both VMs
  - › **Defender for SQL**: Vulnerability scans + threat alerts
- **Just-In-Time (JIT) Access**:
  - › RDP/SQL ports open **only when requested** — auto-closed after 1 hour
- **Azure Monitor + Log Analytics**:
  - › IIS logs → failed requests, 500 errors
  - › SQL logs → failed logins, slow queries
  - › **Alerts** fire on suspicious patterns (e.g., SQL injection from web tier)



## Secure IIS & ASP.NET Hardening

- **IIS** is hardened:
  - › **Request Filtering** blocks SQLi/XSS
  - › **URLScan** rejects malicious patterns
  - › **AppPool** identity runs as low-privilege
- **ASP.NET:**
  - › ViewStateEncryptionMode="Always"
  - › Anti-forgery tokens on all forms
  - › MS Identity Framework Auth + Azure AD integration
- **WAF via Application Gateway:**
  - › OWASP CRS 3.2 ruleset
  - › Blocks bad bots, injection attempts



## SQL Server on Dedicated VM – Locked Down

- **Private Endpoint** only — **no public IP**
- **Auditing** logs all queries from IIS V



## Automated Compliance & Patching

- **Our Azure Policy** enforces:
  - › No public SQL
  - › Disk encryption
  - › Defender enabled
- **Our Azure Update Manager Policy:**
  - › Auto-patches Windows + SQL monthly
  - › Pre-approved critical updates

## Result: Zero Trust, Total Visibility

Previstar CPS delivers a true zero-trust security posture with comprehensive visibility and robust controls at every layer.

| LAYER            | STATUS                       |
|------------------|------------------------------|
| Network          | Isolated + WAF               |
| Identity         | Azure AD + RBAC              |
| Data             | Encrypted at rest/in transit |
| Threat Detection | Real-time + JIT              |
| Compliance       | Audit-ready                  |

Operational Readiness  
is Continuous.

[SummitET.com/Previstar](https://SummitET.com/Previstar)